Information Technology Security Requirements Summary

1. Background Investigation

Contractor employees who will have access to federal information technology (IT) systems are subject to background investigations by the Federal Office of Personnel Management. Procedures for investigations and obtaining identity credentials are described in clause GS1414. The level of investigation required will be the same as would be required for federal employees holding positions involving similar duties.

Based on the risk and sensitivity of duties performed and system access authorities to be granted, the following type of background investigations will be required, as described in DOI Departmental Manual Part 441, Chapter 3, Attachment 5 (available at: http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3631).

2. Non-disclosure Agreement

Prior to receiving access to USGS computers, contractor employees shall be required to sign nondisclosure or other system security agreements, depending on the systems to be used and level of access granted. Restrictions on use, duplication and disclosure of sensitive and proprietary data are covered in clause GS1406.

Work under this contract may involve design, development, or operation of (access to) systems containing personal information protected by the Privacy Act (5 U.S.C. Section 552a).

The contractor will not be required or permitted to respond to requests for Privacy Act data or to make decisions about releases of data under the Act. Contractor will ensure its employees are instructed to safeguard against improper use or release of such data and advise them that violation of the Act may involve criminal penalties. The contractor will comply with FAR clause 52.224-2, Privacy Act, incorporated herein by reference, and with DOI Privacy Act regulations at 43 CFR 2, Subpart D, available at: http://www.doi.gov/foia/43cfrsub.html .

3. Training

Contractor employees shall complete USGS-defined Federal Information Systems Security Awareness computer security training before being granted system access and must renew the training annually. Failure to complete training within the required timeframe may result in loss of system access for that user. Contractor employees with significant IT security responsibilities shall also complete specialized role-based training.

4. Personnel Changes

Before starting work, the contractor will provide a listing to the COR/technical liaison identifying contractor and subcontractor employees requiring access to USGS systems for performance of work hereunder and will assign each person a unique user ID conforming to USGS policy in Survey Manual Chapter 600.2.1. The contractor shall immediately advise the

USGS Project Officer when any of their personnel no longer require USGS computer access so that those ID's and access privileges can be cancelled. When possible, the COR must be notified in advance of any potentially unfriendly termination of an employee or subcontractor.

5. Contractor Location

No portion of the services to be performed hereunder may be performed outside the United States without the express written permission of the Contracting Officer. If a contractor proposes to perform services outside the United States, the contractor must submit a Security Plan to address mitigation of security issues due specifically to location. The Security Plan Template is available upon request from the Contracting Officer. Such proposals will not be accepted unless the contractor can demonstrate that the Government systems or data would be no more vulnerable than if work were performed domestically.

6. Applicable Standards

Contractors shall follow the DOI System Development Life Cycle (SDLC), NIST SP800-64, and the DOI SDLC Security Integration Guide or similar methodology as determined appropriate by the applicable Government system owner/program manager. NIST SP800-64 is available at http://csrc.nist.gov/publications/nistpubs/index.html, DOI SDLC and DOI SDLC Security Integration Guide will be provided by the Contracting Officer, upon request.

7. Asset Valuation

Asset valuation on USGS systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors.

8. Property Rights

The Government shall be granted unlimited rights in software or data produced hereunder as described in FAR clause 52.227-17, Rights in Data—Special Works, incorporated by reference herein.

9. Independent Verification and Validation (IV & V)

In the development or maintenance of custom applications, software will be independently verified and validated using a methodology determined appropriate by the Government system owner/program manager prior to being moved into production.

Contractor will ensure that independent verification and validation, as deemed appropriate by the applicable Government system owner/program manager, is performed on software deployed on contractor managed systems containing USGS data, in accordance with DOI SDLC Security Integration Guide or similar methodology.

10. Certification & Accreditation

The contractor will perform Certification and Accreditation (C&A) services on the application developed or maintained hereunder prior to going into production. The application must be re-accredited every three years or whenever there is a major change that affects security as determined by the Government system owner. C&A documents will be provided to the COR in both hard copy and electron forms. The contractor must follow NIST SP 800-37, 800-18, 800-30, 800-60 800-53A, Federal Information Processing Standard (FIPS) 199 and 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment. NIST documents are available on the Internet at http://csrc.nist.gov/publications/nistpubs/. FIPS documents are available the internet at http://csrc.nist.gov/publications/nistpubs. The contractor may request copies of DOI documents by contacting the Contracting Officer.

The Government reserves the right to conduct the ST&E, using either Government personnel or an independent contractor.

With the approval of the Government system owner, the contractor will take immediate and timely action to correct or mitigate any weaknesses discovered, as necessary, to bring the application or system into compliance with the above requirement.

Certification and Accreditation on USGS systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors

With the knowledge and approval of the Government system owner, the Contractor must maintain systems that are compliant with NIST SP 800-18, 800-30, 800-37, 800-53A, 800-60, Federal Information Processing Standard (FIPS) 199 and 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment.

As required by the above, Major Applications and General Support Systems shall be certified and accredited (C&A) prior to going into production and re-accredited every three years or whenever there is a major change that affects security. C&A documents will be provided to the COR in both hard copy and electronic forms.

NIST documents are available on the internet at http://csrc.nist.gov/publications/nistpubs/. The contractor may request copies of DOI documents by contacting the Contracting Officer.

The government will reserve the right to conduct the ST&E, using either Government personnel or an independent contractor.

The contractor will take immediate and timely action to correct or mitigate any weaknesses discovered as necessary to bring the application or system into compliance with the above requirement.

11. Internet Logon Banner

Web-based applications developed or maintained under this contract must contain a USGS approved logon banner. See http://internal.usgs.gov/gio/security/doi_2001-005_banner.pdf

12. Incident Reporting

Contractor employees must report any computer security incidents (viruses, intrusion attempts, system compromises, offensive e-mail, etc.) which may affect Government data or systems in accordance with the DOI Computer Incident Response Guide and local reporting procedures. Report computer security incidents to USGS help desk or Security Point Of Contact (SPOC). In many cases, your local system administrator is your Security Point Of Contact. The help desk or SPOC will investigate and coordinate with the Computer Security Incident Response Team (CSIRT)

13. Quality Control (Malicious Code)

All software and hardware shall be free of malicious code.

14. Self Assessment

Except as provided below, self-assessment on USGS systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors.

The contractor shall conduct an annual self assessment in accordance with NIST SP 800-26 on major applications and General Support Systems operated or maintained under this contract and on any outsourced applications in production, or other off-site systems used by the contractor for performance under this contract. NIST documents are available on the Internet at http://csrc.nist.gov/publications/nistpubs/. Both hard copy and electronic copies of the assessment will be provided to the COR

The government will reserve the right to conduct such an assessment using Government personnel or another contractor.

With the knowledge and concurrence of the Government system owner; the contractor will take immediate action to correct or mitigate any weaknesses discovered during such testing to ensure that all systems meet security standards specified elsewhere in the work statement.

15. Vulnerability Analysis

Vulnerability Analysis on USGS systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors.

All systems operated and managed by the contractor shall be scanned monthly with a vulnerability analysis tool provided by the Government. All “safe” or “non-destructive” checks must be turned on. All electronic copies of each report and session data shall be provided to the COR.

The Government may conduct additional independent vulnerability scans, prearranged or unannounced. All high risk systems and systems accessible from the Internet will be tested for penetration. Independent testing may be performed by the Government or by another contractor.

With the knowledge and concurrence of the Government system owner; the contractor shall take immediate action to correct or mitigate any weaknesses discovered during any vulnerability

testing, as needed, to bring the system into compliance with security standards invoked elsewhere in this work statement.

The contractor will perform security testing on designated USGS/DOI systems using testing techniques described in NIST SP800-42, Guidelines on Network Security Testing, including vulnerability analysis and penetration testing. When DOI provides the testing tool, all "safe" and "non-destructive" checks must be turned on. All electronic copies of each report and session data shall be provided to the applicable Government system owner.

16. Logon Banner

Applications developed or maintained under this contract must contain a USGS approved logon warning advising users of rules, restrictions, and privacy expectations for that application. The text of such warning will be provided by the Government system owner.

When presented with the USGS logon banner, contractor employees shall read and acknowledge a Government approved logon warning.

17. Security Controls

In the development or maintenance of custom applications, the contractor shall, with the knowledge and concurrence of the Government system owner, be responsible for Information Technology (IT) security for all non-government-owned systems used in the development of and systems intended for eventual delivery to the USGS/DOI in fulfillment of contract requirements. This includes IT, hardware, software, databases, networks, and telecommunications systems.

Security functionality in applications or integrated systems delivered hereunder must operate with the Government systems on which or with which it will eventually be deployed. Products delivered hereunder must not cause misoperation of government resources or loss of integrity, confidentiality, or availability of electronic information or data.

The Contractor shall ensure compliance with the security control requirements of the current version of NIST SP 800-53 and FIPS 200 appropriate to the sensitivity and criticality of the application/system assigned by the Government based on FIPS 199 and the DOI Asset Valuation Guide. NIST documents are available on the internet at http://csrc.nist.gov/publications/nistpubs/. FIPS documents are available on the internet at http://csrc.nist.gov/publications/nistpubs/. DOI documents will be provided by the Contracting Officer upon request.

The Contractor shall be responsible for IT security for all contractor-operated systems connected to a USGS/DOI network, regardless of location. The Contractor shall ensure compliance with the security control requirements of current version of NIST SP 800-53 and FIPS 200 appropriate to the sensitivity and criticality of the application/system. FIPS 199 and the DOI Asset Valuation Guide shall be used to determine the applications/systems sensitivity and criticality. NIST documents are available on the Internet at http://csrc.nist.gov/publications/nistpubs/. FIPS documents are available on the Internet at http://csrc.nist.gov/publications/nistpubs/. DOI documents will be provided by the Contracting Officer, upon request.

18. Contingency Plan

The Contractor shall submit a contingency plan for restoration and testing of software and resumption of maintenance support during a contingency operation. The plan must conform to applicable portions of NIST SP 800-34 and DOI Contingency Plan Guide and be consistent with existing EROS continuity of operation procedures and plans. The Contractor shall submit contingency plans to the applicable Government system owner. NIST documents are available on the Internet at http://csrc.nist.gov/publications/nistpubs/. The contractor can request copies of the DOI Contingency Plan Guide by contacting the Contracting Officer.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.]

Other Contractor Employees without Significant IT Security Responsibilities – Moderate or Low Risk

Work Statement Attachment - Information Technology Security Requirements

1. Background Investigation

Contractor employees who will have access to Federal information technology (IT) systems are subject to background investigations by the Federal Office of Personnel Management. The level of investigation required will be the same as would be required for Federal employees holding positions involving similar duties. DM441, Chapter 3, provides guidance for the appropriate background investigations based on types of access, see http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3631.

Investigation Level will be determined by the COR. Moderate Risk positions would require a Minimum Background Investigation (MBI) with Credit Check. Low Risk positions would require a National Agency Check with Inquiries (NACI) with Credit Check. The government will initiate, sponsor and pay for the necessary background investigations. Contractors cannot gain access to USGS systems until the NAC has been favorably adjudicated.

2. Non-disclosure Agreement

Prior to receiving access to DOI/USGS computers, contractor employees will be required to sign nondisclosure or other system security agreements. The required non-disclosure agreement will be similar to the attached but may be customized as needed to reflect the data involved.

3. Training

Contractor employees must successfully complete DOI's end-user computer security awareness training prior to being granted access to DOI/USGS systems or data or being issued a user account. Training must be renewed annually. Additionally, the contract employees must sign a Statement of Responsibility (SOR) that states they have read the appropriate Rules of Behavior and other applicable Information security policies. Failure to complete training within the required timeframe will result in loss of system access for that user. Contractor employees with significant IT security responsibilities shall also complete specialized role-based training annually.

4. Personnel Changes

Before starting work, the contractor will provide a listing to the COR/technical liaison identifying contractor and subcontractor employees requiring access to DOI/USGS systems for performance of work. The contractor must notify the COR immediately when an employee working on a DOI/USGS system is reassigned or leaves the contractor's employ. For unfriendly terminations, the COR must be contacted PRIOR to the termination, as is practicable. The Bureau/Office Security Officer should also be notified.

5. Contractor Location

These are on-site services, see location(s) in the Statement of Work.

6. Applicable Standards

Not Applicable

7. Security Categorization

Security Categorization for systems the contractor may access is the responsibility of the Government.

8. Property Rights

The Government shall be granted unlimited rights in software or data produced hereunder as described in FAR clause 52.227-17, Rights in Data—Special Works, incorporated by reference herein.

9. Independent Verification and Validation (IV & V)

Not Applicable.

10. Certification & Accreditation (C&A)

C & A for systems the contractor may access is the responsibility of the Government.

11. Internet Logon Banner

Not Applicable.

12. Incident Reporting

Contractor employees must report any computer security incidents (viruses, intrusion attempts, system compromises, offensive e-mail, etc.) which may affect Government data or systems in accordance with the *DOI Computer Incident Response Guide*. The DOI Computer Incident Response Guide will be provided upon request.

13. Quality Control (Malicious Code)

Not Applicable.

14. Self Assessment

Self Assessment on systems the contractor may access is the responsibility of the Government.

15. Vulnerability Analysis

Vulnerability Analysis on systems the contractor may access is the responsibility of the Government.

16. Logon Banner

Contractor employees who access DOI information systems must acknowledge a government-approved legal warning banner prior to logging on to the system.
The network warning banner communicates that there is no expectation of privacy in the authorized or unauthorized use of DOI information systems. The use of warning banners on DOI computers and networks provides legal notice to anyone accessing them that they are using a U.S. Government system that is subject to monitoring. Users should also be notified of the possible sanctions, such as loss of privileges or prosecution, if they misuse or access the network without authorization. All DOI computers, workstations, laptops and other information resources will display a standard, DOI approved legal banner.

17. Security Controls

Not Applicable.

18. Contingency Plan

Contingency Planning on systems the contractor may access is the responsibility of the Government.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.]

System Administrators and Data Base Administrators - Moderate Risk

Work Statement Attachment - Information Technology Security Requirements

1. Background Investigation

Contractor employees who will have access to Federal information technology (IT) systems are subject to background investigations by the Federal Office of Personnel Management. The level of investigation required will be the same as would be required for Federal employees holding positions involving similar duties. DM441, Chapter 3, provides guidance for the appropriate background investigations based on types of access, see http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3631.

Investigation Level – moderate risk. This level requires a Minimum Background Investigation (MBI) with Credit Check. The government will initiate, sponsor and pay for the necessary background investigations. Contractors cannot gain access to USGS systems until the NAC has been favorably adjudicated.

2. Non-disclosure Agreement

Prior to receiving access to DOI/USGS computers, contractor employees will be required to sign nondisclosure or other system security agreements. The required non-disclosure agreement will be similar to the attached but may be customized as needed to reflect the data involved.

3. Training

Contractor employees must successfully complete DOI's end-user computer security awareness training prior to being granted access to DOI/USGS systems or data or being issued a user account. Training must be renewed annually. Additionally, the contract employees must sign a Statement of Responsibility (SOR) that states they have read the appropriate Rules of Behavior and other applicable Information security policies. Failure to complete training within the required timeframe will result in loss of system access for that user. Contractor employees with significant IT security responsibilities shall also complete specialized role-based training annually.

4. Personnel Changes

Before starting work, the contractor will provide a listing to the COR/technical liaison identifying contractor and subcontractor employees requiring access to DOI/USGS systems for performance of work. The contractor must notify the COR immediately when an employee working on a DOI/USGS system is reassigned or leaves the contractor's employ. For unfriendly terminations, the COR must be contacted PRIOR to the termination, as is practicable. The Bureau/Office Security Officer should also be notified.

5. Contractor Location

These are on-site services, see location(s) in the Statement of Work.

6. Applicable Standards

Not Applicable.

7. Security Categorization

Security Categorization is the responsibility of the government, however contractor personnel shall be involved as required. The Contractor shall follow the FIPS 199 and the NIST SP 800-60 for systems to determine information types and security categorization based on mission impact, data sensitivity, risk level, and bureau / departmental / national criticality. See http://csrc.nist.gov/publications/

8. Property Rights

The Government shall be granted unlimited rights in software or data produced hereunder as described in FAR clause 52.227-17, Rights in Data—Special Works, incorporated by reference herein.

9. Independent Verification and Validation (IV & V)

Software updates must be independently verified and validated by the Government or another Government contractor prior to being moved into production.

10. Certification & Accreditation (C&A)

Major Applications and General Support Systems must be certified and accredited (C&A) prior to going into production and reaccredited every three years or whenever there is a major change that affects security.

The Government has the overall responsibility for C&A, however contractor personnel shall be involved as required. The contractor shall follow NIST SP 800-37, 800-18, Rev.1, 800-30, 800-60 vol. 1 and vol. 2, 800-53, Rev.3, Annex 1, Annex 2 and Annex 3, FIPS 199 and FIPS 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment. See http://csrc.nist.gov/publications/

The government will reserve the right to conduct the ST&E, using either government personnel or an independent contractor. The contractor will take appropriate and timely action to correct or mitigate any weaknesses discovered during such testing.

The authorizing official (Designated Approving/Accrediting Authority) for the system will be the official identified in DOI Secretarial Order No. 3255.

11. Internet Logon Banner

A DOI-approved internet logon banner must be displayed on the first page of any publicly accessible web pages owned by DOI.

12. Incident Reporting

Contractor employees must report any computer security incidents (viruses, intrusion attempts, system compromises, offensive e-mail, etc.) which may affect Government data or systems in

accordance with the *DOI Computer Incident Response Guide*. The DOI Computer Incident Response Guide will be provided upon request.

13. Quality Control (Malicious Code)

All software must be free of malicious code such as viruses, Trojan horse programs, worms, spyware, etc Malicious code or malware is defined as software (or firmware) designed to damage or do other unwanted actions on a computer system.

14. Self Assessment

The government has the responsibility for Self Assessment, however contractor personnel shall be involved as required and/or take appropriate and timely action to correct or mitigate any weaknesses discovered.

15. Vulnerability Analysis

The government has the responsibility for Vulnerability Analysis, however contractor personnel shall be involved as required and/or take appropriate and timely action to correct or mitigate any weaknesses discovered.

All systems must be scanned monthly with a vulnerability analysis tool that is compatible with the software in use by the OCIO at the time (specify this in the solicitation). All "safe" or "non-destructive" checks must be turned on.

At least annually, all high and moderate risk impact systems and systems accessible from the Internet must be independently penetration tested.

16. Logon Banner

Contractor employees who access DOI information systems must acknowledge a government-approved legal warning banner prior to logging on to the system.
The network warning banner communicates that there is no expectation of privacy in the authorized or unauthorized use of DOI information systems. The use of warning banners on DOI computers and networks provides legal notice to anyone accessing them that they are using a U.S. Government system that is subject to monitoring. Users should also be notified of the possible sanctions, such as loss of privileges or prosecution, if they misuse or access the network without authorization. All DOI computers, workstations, laptops and other information resources will display a standard, DOI approved legal banner.

17. Security Controls

Contractors will be required to ensure compliance with the security control requirements of the current version of NIST SP 800-53, Rev.3, which are applicable to the security categorization of the data or system. FIPS 199 and the NIST SP 800-60 will be used to determine information types and security categorizations. See http://csrc.nist.gov/publications/

18. Contingency Plan

The government has the responsibility for Contingency Planning, however contractor personnel shall be involved as required. The contractor shall follow NIST SP 800-34 and the DOI Contingency Plan Guide. The DOI Contingency Plan Guide will be provided upon request for NIST documents see http://csrc.nist.gov/publications/

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.]

Software Developers & Software Engineers - Moderate Risk

Work Statement Attachment - Information Technology Security Requirements

1. Background Investigation

Contractor employees who will have access to Federal information technology (IT) systems are subject to background investigations by the Federal Office of Personnel Management. The level of investigation required will be the same as would be required for Federal employees holding positions involving similar duties. DM441, Chapter 3, provides guidance for the appropriate background investigations based on types of access, see http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3631.

Investigation Level – moderate risk. This level requires a Minimum Background Investigation (MBI) with Credit Check. The government will initiate, sponsor and pay for the necessary background investigations. Contractors cannot gain access to USGS systems until the NAC has been favorably adjudicated.

2. Non-disclosure Agreement

Prior to receiving access to DOI/USGS computers, contractor employees will be required to sign nondisclosure or other system security agreements. The required non-disclosure agreement will be similar to the attached but may be customized as needed to reflect the data involved.

3. Training

Contractor employees must successfully complete DOI's end-user computer security awareness training prior to being granted access to DOI/USGS systems or data or being issued a user account. Training must be renewed annually. Additionally, the contract employees must sign a Statement of Responsibility (SOR) that states they have read the appropriate Rules of Behavior and other applicable Information security policies. Failure to complete training within the required timeframe will result in loss of system access for that user. Contractor employees with significant IT security responsibilities shall also complete specialized role-based training annually.

4. Personnel Changes

Before starting work, the contractor will provide a listing to the COR/technical liaison identifying contractor and subcontractor employees requiring access to DOI/USGS systems for performance of work. The contractor must notify the COR immediately when an employee working on a DOI/USGS system is reassigned or leaves the contractor's employ. For unfriendly terminations, the COR must be contacted PRIOR to the termination, as is practicable. The Bureau/Office Security Officer should also be notified.

5. Contractor Location

These are on-site services, see location(s) in the Statement of Work.

6. Applicable Standards

Contractors must follow the DOI System Development Life Cycle (SDLC), NIST SP 800-64 and the DOI SDLC Security Integration Guide. The DOI SDLC will be provide upon request, NIST documents can be found at http://csrc.nist.gov/publications/

7. Security Categorization

Security Categorization is the responsibility of the government, however as required the Contractor shall use the FIPS 199 and the NIST SP 800-60 for systems to determine information types and security categorization based on mission impact, data sensitivity, risk level, and bureau / departmental / national criticality. See http://csrc.nist.gov/publications/

8. Property Rights

The Government shall be granted unlimited rights in software or data produced hereunder as described in FAR clause 52.227-17, Rights in Data—Special Works, incorporated by reference herein.

9. Independent Verification and Validation (IV & V)

Software updates must be independently verified and validated by the Government or another Government contractor prior to being moved into production.

10. Certification & Accreditation (C&A)

Major Applications and General Support Systems must be certified and accredited (C&A) prior to going into production and reaccredited every three years or whenever there is a major change that affects security.

The Government has the overall responsibility for C&A on systems the contractor may access. However, if requested to assist the contractor shall follow NIST SP 800-37, 800-18, Rev.1, 800-30, 800-60 vol. 1 and vol. 2, 800-53, Rev.3, Annex 1, Annex 2 and Annex 3, FIPS 199 and FIPS 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment. See http://csrc.nist.gov/publications/

The government will reserve the right to conduct the ST&E, using either government personnel or an independent contractor. The contractor will take appropriate and timely action to correct or mitigate any weaknesses discovered during such testing.

The authorizing official (Designated Approving/Accrediting Authority) for the system will be the official identified in DOI Secretarial Order No. 3255.

11. Internet Logon Banner

A DOI-approved internet logon banner must be displayed on the first page of any publicly accessible web pages owned by DOI.

12. Incident Reporting

Contractor employees must report any computer security incidents (viruses, intrusion attempts, system compromises, offensive e-mail, etc.) which may affect Government data or systems in

accordance with the *DOI Computer Incident Response Guide*. The DOI Computer Incident Response Guide will be provided upon request.

13. Quality Control (Malicious Code)

All software must be free of malicious code such as viruses, Trojan horse programs, worms, spyware, etc Malicious code or malware is defined as software (or firmware) designed to damage or do other unwanted actions on a computer system.

14. Self Assessment

The government has the responsibility to conduct the Self Assessment using Government personnel or contractors. If requested, the contractor shall assist and/or take appropriate and timely action to correct or mitigate any weaknesses discovered.

15. Vulnerability Analysis

The government has the responsibility to conduct the Vulnerability Analysis using Government personnel or contractors. If requested, the contractor shall assist and/or take appropriate and timely action to correct or mitigate any weaknesses discovered.

All systems must be scanned monthly with a vulnerability analysis tool that is compatible with the software in use by the OCIO at the time (specify this in the solicitation). All "safe" or "non-destructive" checks must be turned on.

At least annually, all high and moderate risk impact systems and systems accessible from the Internet must be independently penetration tested.

16. Logon Banner

Contractor employees who access DOI information systems must acknowledge a government-approved legal warning banner prior to logging on to the system.
The network warning banner communicates that there is no expectation of privacy in the authorized or unauthorized use of DOI information systems. The use of warning banners on DOI computers and networks provides legal notice to anyone accessing them that they are using a U.S. Government system that is subject to monitoring. Users should also be notified of the possible sanctions, such as loss of privileges or prosecution, if they misuse or access the network without authorization. All DOI computers, workstations, laptops and other information resources will display a standard, DOI approved legal banner.

17. Security Controls

Contractors will be required to ensure compliance with the security control requirements of the current version of NIST SP 800-53, Rev.3, which are applicable to the security categorization of the data or system. FIPS 199 and the NIST SP 800-60 will be used to determine information types and security categorizations. See http://csrc.nist.gov/publications/

18. Contingency Plan

The government has the responsibility to conduct Contingency Planning using Government personnel or contractors. If requested, the contractor shall assist and be compliant with NIST SP 800-34 and the DOI Contingency Plan Guide. The DOI Contingency Plan Guide will be provided upon request for NIST documents see http://csrc.nist.gov/publications/

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.]